Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF COMCAST CORPORATION

Matthew T. Murchison
Alexander L. Stout
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

Mitch Rose
Jordan Goldstein
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

December 10, 2021

TABLE OF CONTENTS

Page

INTRODUCTION AND SUMMARY 1

DISCUSSION 2

I. THE COMMISSION SHOULD CAREFULLY CONSIDER HOW BEST TO ADDRESS THE ROLE OF GATEWAY PROVIDERS 2

II. COMCAST STRONGLY SUPPORTS EXTENDING STIR/SHAKEN CALLER ID AUTHENTICATION REQUIREMENTS TO GATEWAY PROVIDERS 4

III. THE COMMISSION SHOULD CONTINUE TO EXAMINE WHAT OTHER ROBOCALL MITIGATION REQUIREMENTS SHOULD BE APPLIED TO ADDRESS GATEWAY-RELATED ISSUES 7

CONCLUSION 12

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF COMCAST CORPORATION

Comcast Corporation ("Comcast") submits these comments in response to the Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 and the Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 released on October 1, 2021.[1]

INTRODUCTION AND SUMMARY

Comcast strongly supports the Commission's continuing efforts to address the problem of illegal and fraudulent robocalls, and the latest *FNPRM* is yet another step forward as the Commission works to empower voice providers to implement effective call blocking tools. The Commission's adoption of the *FNPRM* underscores its commitment to continuing the significant progress made in recent years to mitigate harmful robocalls, this time by proposing important measures to stop illegal calls using domestic telephone numbers that originate outside the United States. By extending call blocking and call authentication requirements to so-called "gateway providers," the Commission can reduce the flow of harmful foreign calls into our nation's voice networks. Such measures would enhance the effectiveness of the Commission's broader

---

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 and the Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105 (rel. Oct. 1, 2021) ("*FNPRM*").

robocall mitigation initiatives by ensuring that gateway providers participate fully in call blocking and call authentication efforts.

Moving forward, the Commission should adopt measures in response to the *FNPRM* that would build off past successes. Comcast agrees with the Commission that its "current rules addressing foreign-originated robocalls are not sufficient to resolve the problem of foreign-originated illegal robocalls," and that this problem warrants consideration of further regulatory efforts targeting gateway providers that route such calls along to the U.S. public switched telephone network.[2] Comcast accordingly supports the Commission's proposal to extend STIR/SHAKEN implementation and verification requirements to gateway providers. The Commission has long recognized that STIR/SHAKEN is the best tool available to combat spoofed robocalls, and Comcast strongly supports efforts to expand the reach of STIR/SHAKEN to as many providers in the call path as possible. The Commission also should pursue certain other proposals in the *FNPRM* aimed at making gateway providers part of the solution to the problem of illegal robocalls, such as adopting appropriately tailored call blocking mandates, encouraging "know-your-customer" programs for upstream providers, and expanding participation in the Robocall Mitigation Database.

DISCUSSION

I. THE COMMISSION SHOULD CAREFULLY CONSIDER HOW BEST TO ADDRESS THE ROLE OF GATEWAY PROVIDERS

In the *FNPRM*, the Commission proposes to require gateway providers to apply STIR/SHAKEN caller ID authentication to, and perform robocall mitigation on, foreign-originated calls with U.S. numbers.[3] The Commission also proposes several additional robocall

[2] *Id.* ¶ 24.

[3] *Id.* ¶ 40.

mitigation requirements for gateway providers, each with the aim of preventing illegal calls that originate abroad and use U.S. telephone numbers from entering the U.S. telephone system. Comcast generally supports the Commission's consideration of such initiatives.

Today, the Commission's rules require gateway providers that bring foreign calls into the United States to pass unaltered call authentication information to the next provider down the chain, participate in traceback efforts, and take steps to mitigate illegal traffic effectively when notified of such traffic by the Commission.[4] These requirements are important, but incomplete. As the Commission has recognized, foreign-originated spoofed robocalls continue to plague Americans by displaying a U.S. number in the caller ID field that implies to the call recipient that the call originated in the United States.[5] Under the current rules, so long as these calls arrive at the gateway provider's network without STIR/SHAKEN authentication, gateway providers can simply pass those completely unauthenticated calls deeper into the U.S. telephone system. Unfortunately, the foreign voice service providers that are the originators of these calls are generally beyond the reach of the Commission's rules, and so many foreign-originated calls bound for the United States go unauthenticated as a result—a hole that the Commission is appropriately seeking to plug by proposing authentication obligations for gateway providers in this proceeding. Moreover, while gateway providers' current obligations to respond to traceback requests and to respond to Commission notifications of unlawful traffic are significant and beneficial, they are largely *reactive* in nature, and cannot take the place of *proactive* duties to mitigate harmful traffic directed towards the United States from abroad. The proposed measures discussed below would go a long way towards making gateway providers more active

---

[4] *See id.* ¶ 16.

[5] *See id.* ¶¶ 4-5.

participants in efforts to stem the tide of illegal foreign-originated robocalls bound for U.S. consumers.

In considering these measures, the Commission also should refrain from assuming that all gateway providers are necessarily bad actors. To be sure, in recent years, the Commission has identified numerous gateway providers that have allegedly facilitated the delivery of foreign-originated fraudulent robocalls to U.S. consumers, and has taken appropriate enforcement action against those providers in coordination with the Federal Trade Commission, the Department of Justice, and other law enforcement bodies.[6] But the Commission should bear in mind that these findings about particular gateway providers might not apply to all gateway providers, particularly if the Commission ultimately adopts an expansive definition of the term "gateway provider." The proposals from the *FNPRM* discussed below, in Comcast's view, appropriately balance the need for action with the recognition of this nuance.

II. COMCAST STRONGLY SUPPORTS EXTENDING STIR/SHAKEN CALLER ID AUTHENTICATION REQUIREMENTS TO GATEWAY PROVIDERS

Comcast strongly supports the Commission's proposal to require gateway providers to apply STIR/SHAKEN-compliant attestation to unsigned SIP calls bound for the United States and carrying a U.S. number in the caller ID field.[7] Comcast agrees with the Commission that expanding STIR/SHAKEN obligations across the voice service ecosystem will benefit all parties and call recipients. While call authentication may not be a panacea, it is a critical step in reestablishing Americans' trust in the telephone system.[8]

---

[6] *See id.* ¶¶ 28-29 & n.91.

[7] *See id.* ¶ 38.

[8] *See* Questions for the Record, Jessica Rosenworcel, Federal Communications Commission, S. Comm. on Commerce, Science & Transportation, 117th Cong., 24,

As an early adopter and proponent of STIR/SHAKEN, Comcast is especially supportive of extending call authentication implementation obligations to gateway providers. As the Commission is aware, Comcast was one of only a handful of providers that demonstrated substantial early progress in implementing STIR/SHAKEN by December 2020,[9] and in June 2021, Comcast demonstrated that it had completed full implementation of the STIR/SHAKEN protocol on its network in accordance with its prior commitments.[10] Moreover, as Comcast's prior submissions reflect, a growing number of calls originating from other providers and bound for Comcast's customers are signed and verified.[11] That number will continue to increase with broader adoption and implementation of the STIR/SHAKEN protocol across the industry. While Comcast believes the effectiveness of STIR/SHAKEN should speak for itself, where necessary, the Commission should continue to use its regulatory authority to ensure that STIR/SHAKEN is fully adopted and properly utilized by all providers in the United States.

Comcast also broadly agrees with the specific STIR/SHAKEN requirements that the Commission proposes to adopt for gateway providers. In the *FNPRM,* the Commission proposes to require a gateway provider to "authenticate caller ID information for SIP calls it receives for which the caller ID information has not been authenticated and which it will exchange with

---

https://www.commerce.senate.gov/services/files/E4FB6E39-28F0-4328-902A-04F5F511825C ("The agency is also working to require providers that serve as a gateway for foreign-originated calls to participate in the STIR/SHAKEN framework. This is essential because we understand that a large number of these junk calls are now originating overseas.").

[9] *See Wireline Competition Bureau Announces Seven Voice Service Providers Qualified for STIR/SHAKEN Exemption*, Public Notice, 35 FCC Rcd 14830 (WCB 2020).

[10] *See* Comcast Corp., Caller ID Authentication Exemption Verification Certification, WC Docket No. 20-68 (filed Oct. 4, 2021).

[11] *See, e.g.*, Letter of Charles Herrin, Comcast Corp., to G. Patrick Webre, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 3 (filed Apr. 30, 2021).

another provider as a SIP call."[12] The *FNPRM* also proposes that gateway providers use the ATIS-1000074, ATIS-1000080, and ATIS-1000084 standards for this purpose.[13] Comcast agrees that these standards are correct and appropriate for the Commission's envisioned use. The Commission also is correct in declining to predetermine the attestation level that gateway providers may assign to a given call.[14] In Comcast's experience, C-level "gateway" attestation likely will be the appropriate attestation level for gateway providers in most cases, but providers should not be limited and should have the flexibility to apply a higher level of attestation if and where possible. There is no reason to prohibit providers from assigning higher levels of attestation where they possess the information and confidence necessary to do so.

Finally, because the STIR/SHAKEN protocols are reliant on IP-based standards, the Commission should do everything it can to facilitate the transition to IP-based networks. Fortunately, in Comcast's experience, most gateway providers already exchange traffic in SIP and therefore likely are ready to implement STIR/SHAKEN. But for those who do not, encouraging them to transition to IP will facilitate IP-to-IP interconnection and enable more widespread adoption and implementation of STIR/SHAKEN. Importantly, no end-to-end caller ID authentication solution for non-IP networks has been deployed in the real world, and the Commission should not require STIR/SHAKEN-compliant providers to accommodate alternative approaches (such as out-of-band STIR) designed for legacy technologies.[15] Efforts to combat illegal spoofed robocalls will be more effective when IP technology is ubiquitous and authentication information can be shared seamlessly across all providers.

---

[12] *FNPRM* ¶ 43.

[13] *Id.* ¶ 44.

[14] *See id.* ¶ 45.

[15] *See id.* ¶ 46.

III. THE COMMISSION SHOULD CONTINUE TO EXAMINE WHAT OTHER ROBOCALL MITIGATION REQUIREMENTS SHOULD BE APPLIED TO ADDRESS GATEWAY-RELATED ISSUES

Comcast supports the Commission's efforts to look beyond STIR/SHAKEN and to consider requiring additional actions by gateway providers to reduce the onslaught of foreign-originated illegal robocalls. As discussed further below, many of these proposals warrant further consideration and analysis and may prove to be worthwhile steps. In particular, Comcast believes that certain of the proposed mandatory blocking requirements and "know your customer" requirements may be effective tools to reduce illegal robocalls, if appropriately tailored. Comcast also supports adopting a requirement for gateway providers to file in the Robocall Mitigation Database. Each of these steps would strengthen the Commission's robocall mitigation efforts by bringing gateway providers under rules similar to those currently in effect for terminating and intermediate providers.

First, the *FNPRM* proposes to impose mandatory blocking requirements with respect to certain foreign-originated illegal robocalls. In particular, the *FNPRM* proposes to (i) "affirmatively require gateway providers to block calls upon receipt of notification from the Commission through its Enforcement Bureau,"[16] (ii) "require the voice service provider or intermediate provider downstream from the gateway provider to block where the Commission determines a particular gateway provider is a bad actor,"[17] (iii) require gateway providers to block calls based on reasonable analytics,[18] and (iv) require gateway providers to block calls purported to originate from numbers on the do-not-originate list.[19] Each of these proposals is

---

[16] *Id.* ¶ 57.

[17] *Id.* ¶ 60.

[18] *Id.* ¶ 66.

[19] *Id.* ¶ 71.

worth considering, with appropriate tailoring to ensure that such requirements will be effective and implementable.

For instance, in exploring these proposals, it is important to recognize that traffic from a provider that serves as a point of entry into the U.S. is often mixed when handed off to downstream providers and may include domestic and otherwise lawful voice traffic. In that case, it may be difficult for gateway providers to segregate and block certain calls they carry based on the calls' source, and it would be particularly difficult—if not impossible—for downstream providers to differentiate mixed traffic received from gateway providers. Accordingly, in considering whether to require a downstream provider to block traffic from a gateway provider deemed to be delivering illegal foreign-originated traffic, the Commission should account for the fact that blocking *all* traffic from such a gateway provider could result in the blocking of some domestic and otherwise lawful traffic.

Moreover, in considering whether to mandate blocking based on reasonable analytics for gateway providers, the Commission should be mindful of how such analytics-based tools operate. All analytics-based call blocking is inherently reactive; in order to determine that a call pattern is likely illegal, a provider using reasonable analytics must first observe (and complete) a certain number of calls that trigger pattern-based blocking. In other words, even the best call analytics are likely to "allow" some number of bad actor calls to be completed. Any mandate thus should acknowledge and account for this fact.

The Commission also should adopt a clear and broad safe harbor to protect providers from any liability for implementing mandatory call blocking, including where a downstream voice service provider is required to block all traffic from an upstream gateway provider. In particular, since providers often play different roles for different calls (e.g., as a gateway provider for some calls and as a terminating provider for other calls), the Commission should ensure that any such safe harbor covers providers that reasonably believe the mandatory blocking requirement applies to a given call. Providers should not be penalized for taking action to block calls when they reasonably believe themselves to be acting according to Commission requirements.

Second, the *FNPRM* wisely proposes to impose a "know your customer" requirement for gateway providers. It is critical, however, to ensure that any such requirement is achievable and effective, and does not impose standards on gateway providers that they could not reasonably be expected to meet. In particular, the *FNPRM*'s proposal to require gateway providers to "confirm that a foreign call originator is authorized to use a particular U.S. number that purports to originate the call," likely would pose significant practical challenges that would complicate, if not preclude, compliance.[20] While some gateway providers may have direct relationships to callers or their originating voice service providers, that is often not the role that gateway providers play. Indeed, in many cases the gateway provider is multiple hops from the originating caller or originating network. With one or more intermediate providers carrying traffic to the gateway provider, the gateway provider often has little if any visibility into the identity of the foreign call originator. Moreover, the gateway provider often has no contractual relationship with the foreign call originator, preventing any effort to impose compliance requirements through contract. The same considerations militate against the proposal to "consider the call originator the gateway provider's 'customer' for purposes of such a requirement."[21] A more reasonable and implementable approach would be the Commission's alternative proposal to

---

[20] *Id.* ¶ 80.

[21] *Id.* ¶ 85.

require gateway providers to take steps to know the upstream providers from which they directly receive traffic, and to take reasonable measures to prevent those providers from transmitting illegal traffic onto U.S. networks.[22] Such an approach would appropriately focus on the direct relationships that gateway providers have with foreign carriers, enabling gateway providers to take concrete steps to obtain information about those foreign carriers before carrying their traffic into the United States.

Third, the *FNPRM* proposes to require gateway providers to submit a certification to the Robocall Mitigation Database describing their implementation of call authentication technology and, as necessary, their robocall mitigation practices.[23] Comcast supports this proposal, which would reasonably extend the database filing requirements to another class of providers—giving the Commission and other service providers broader visibility into the implementation status of gateway providers. These straightforward, easily understood submissions ensure that providers recognize their robocall mitigation obligations, carefully consider their mitigation practices, and provide a point of contact for robocall mitigation issues. Gateway providers should be required to participate in the Robocall Mitigation Database in the same manner as other voice service providers.

Fourth and finally, the Commission should thoughtfully examine the petition for reconsideration filed by CTIA and others regarding the so-called foreign provider prohibition—under which U.S.-based providers are prohibited from accepting traffic using U.S. NANP numbers that is received directly from foreign voice service providers that are not in the

---

[22] *Id.* ¶ 84.

[23] *Id.* ¶ 94.

Robocall Mitigation Database.[24] The petitioners raise reasonable concerns about the widespread blocking of lawful foreign-originated calls, and it is prudent for the Commission to consider the merits of that petition on a complete record. While the Commission examines the questions raised by CTIA, Comcast supports the Commission's decision to suspend enforcement of the foreign provider prohibition to ensure that lawful calls are not being blocked indiscriminately.[25]

---

[24] *See id.* ¶¶ 103-06.

[25] *See id.* ¶ 106.

CONCLUSION

Comcast strongly supports the Commission's efforts to stem the tide of foreign-originated illegal robocalls, including by extending call authentication obligations to gateway providers and by considering the adoption of further robocall mitigation measures. As discussed above, the Commission should carefully assess how to tailor its rules to account for important practical considerations and to protect consumers most effectively from abusive foreign-originated calls.

Respectfully submitted,

/s/ Mitch Rose

Mitch Rose
Jordan Goldstein
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

Matthew T. Murchison
Alexander L. Stout
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

December 10, 2021